

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

2018 DEC 28 PM 1:47

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFO. ASSOC. WITH JULOISCHIKA@GMAIL.COM
AND LOGANSIT@GMAIL.COM STORED AT
GOOGLE, LLC

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-1

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section


Offense Description

SEE ATTACHMENT C

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Teddi D. Rachell
 Applicant's signature

 SA TEDDI D. RACHELL, AFOSI
 Printed name and title

Sworn to before me and signed in my presence.

Date:

12/28/18

 Michael J. Newman
 Judge's signature
City and state: DAYTON, OHIO
 MICHAEL J. NEWMAN U.S. MAGISTRATE JUDGE
 Printed name and title

ATTACHMENT A-1

PLACE TO BE SEARCHED

This warrant applies to stored information associated with **juloischika@gmail.com** and **logansit@gmail.com** which is stored and maintained at premises owned, maintained, controlled, or operated by “Google, LLC,” a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B-1

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Google, LLC (the “Provider”):

To the extent the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose, at minimum, the following information to the U.S. Government for each account or identifier listed in Attachment A-1:

- a. The contents of all communications associated with the accounts and all associated Google applications, such as Google Hangouts, from October 9, 2013 to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, chat communications sent to and from the account, the source and destination address associated with each communication, the date and times of all video chats, stored video chat messages and videos, members of video chats who communication with the account including, basic account information and records about their identities;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. Any records related to the possession, receipt, and/or distribution of child pornography;
- e. Any visual depictions of minors;
- f. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- g. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the U.S. Government within ____ days of service of this warrant. The Provider is required to send the requested records

to the Air Force Office of Special Investigations either via their formal legal service database or at the following address:

AFOSI 10 FIS
Attn: SA Teddi Rachell
5215 Thurlow Rd., Bldg. 70
WPAFB, OH 45433

II. Information to be seized by the U.S. Government:

All information described above in Section I of Attachment B-1 which may constitute fruits, contraband, evidence, and instrumentalities of violations of the federal statutes listed on the search warrant involving **LOGAN J. SIT** and occurring on or after October 9, 2013, including, but not limited to, information pertaining to the following matters for each account or identifier listed on Attachment A-1:

- a. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- b. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- c. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- d. The identity of the person(s) who communicated with the user ID,
- e. Communications between the account holder and users known or suspected to be minors;
- f. Records of all individuals with whom the account holder interacted, to include basic account information, user names, contact information, and records which help reveal their whereabouts;
- g. Information related to Internet Protocol (IP) addresses accessed by the account;
- h. Evidence of utilization of aliases and fictitious names;
- i. Evidence of utilization of other email accounts, social media accounts, online chat programs, file storage accounts, including any account or user names;
- j. Financial account statements, telephone records, and billing records;
- k. Information related to the sharing and/or creation of child pornography; and
- l. Communications which relate to the solicitation or inappropriate communications with minors, or soliciting, phishing, or suggesting others for information or assistance in communicating, contacting, or personally meeting with minors.

ATTACHMENT C

FEDERAL CITATIONS

1. 18 U.S.C. § 2252(a)(4)(B) states it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
2. 18 U.S.C. § 2252A(a)(5)(B) states it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
3. 18 U.S.C. § 2252(a)(2)(B) states it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
4. 18 U.S.C. § 2252A(a)(2) states it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
5. 18 U.S.C. § 2422(b) states it is a violation for any person to, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Teddi D. Rachell, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Air Force Office of Special Investigations (AFOSI), and have been so employed since July 2017. I am currently assigned to the 10th Field Investigations Squadron (10 FIS) at Wright-Patterson AFB (WPAFB), OH. I received law enforcement training at the United States Air Force Special Investigations Academy and the Federal Law Enforcement Training Center, both located in Glynco, GA. My primary duties at AFOSI 10 FIS are to conduct criminal, fraud, and counterintelligence investigations where the Department of the Air Force has a vested interest. Since becoming a Special Agent, I have completed the Ohio Internet Crimes Against Children (ICAC) Undercover Chat Course. Prior to joining the Air Force, I attended the University of Missouri – Columbia and graduated in May 2017 with B.A.s in Russian and International Studies.

2. Along with other agents and investigators, I am currently involved in an investigation of offenses described in Attachment C are believed to have been committed by **LOGAN J. SIT** (hereinafter “**SIT**”). This Affidavit is submitted in support of Applications for search warrants for the following:

- a. Information associated with the Google accounts **juloischika@gmail.com** and **logansit@gmail.com** which are stored at premises controlled by Google, LLC (as more fully described in Attachment A-1); and
- b. Information associated with an Amino account which is associated with the email address **juloischika@gmail.com**, user name **banquo0**, and profile address **http://aminoapps.com/p/50nqz2** which are stored at premises controlled by Narvii, Inc. (as more fully described in Attachment A-2).

3. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe violations of the following federal statutes may have been committed by **SIT**: 18 U.S.C. § 2422(b) (Coercion and Enticement), 18 U.S.C. § 2252(a)(4)(B) & (b)(1) (Possession or Attempted Possession of Child Pornography), 18 U.S.C. § 2252A(a)(5)(B) & (b)(1) (Possession or Attempted Possession of Child Pornography), 18 U.S.C. § 2252(a)(2)(B) & (b)(1) (Receipt and Attempted Receipt of Child Pornography), and/or 18 U.S.C. § 2252A(a)(2) & (b)(1) (Receipt and Attempted Receipt of Child Pornography).

4. The purpose of this Application is to seize evidence of suspected violations of these aforementioned statutes (further described in Attachment C). I anticipate executing the requested warrants for the listed accounts under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using said warrants to require Narvii, Inc. and Google, LLC to disclose to the U.S. Government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of said information described in Section I of Attachments B-1 and B-2, U.S. Government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the issuance of the requested search warrants.

6. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

7. As a result of the investigation described more fully below, there is probable cause to believe evidence, fruits, and instrumentalities of violations of federal law further outlined in Attachment C are present within the stored information associated with said accounts (as described in Attachments A-1 and A-2).

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, this Court is a district court (including a magistrate judge) of the United States which has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND INFORMATION

DEFINITIONS

9. The following definitions apply to this Affidavit and any attachments hereto:

- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).
- e. An **“Internet Protocol address,”** also referred to as an **“IP address,”** is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard.

Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session the client computer is connected to the Internet (or other network).

- f. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- g. The terms **"records," "documents,"** and **"materials,"** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- h. **"My Little Pony"** (henceforth **"MLP"**) is a toy line and media franchise intended to target young girls, but has evolved into a global franchise with a cult following of all ages. MLP consists of television shows, movies, and toys which depict multi-colored ponies as humanized characters in a fictional location called Equestria.
- i. A **"pony avatar"** is a fictitious pony persona MLP fans create to identify themselves within the MLP realm. These custom ponies may feature attributes similar to the user, or may be dissimilar and represent a fantasized version of the user.
- j. A **"convention"** is a meeting of people for a common purpose. In the MLP community, there are MLP Conventions which are multi-day events consisting of speakers, concerts, and other MLP-related activities attended by MLP fans of all ages. Many of these MLP Conventions are advertised as "family-friendly" events.
- k. The term **"Brony"** refers to males, primarily teenaged to middle-aged, who have an obsessive love of all things MLP. Bronies have come under much derision in recent years due to their perceived usurpation of MLP. Many families report feeling uncomfortable with the number of teenaged and middle-aged males attending MLP Conferences, as they feel the cartoon and its conferences should be

for the young girls who the show targets. This stigma on the Brony community has led to the creation of several “BronyCons,” which are MLP Conventions which cater to the older male demographic of MLP fans.

1. The “**Dark Web**” is the part of the World Wide Web which is only accessible by means of special software. It allows users and website operators to remain anonymous or untraceable.

COLLECTORS OF CHILD PORNOGRAPHY

10. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):

- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
- b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often maintain companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.
- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

GOOGLE SERVICES

11. Google is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.

12. Google Photos is a photograph and video sharing and storage service provided by Google, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any telephone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.

13. Google+ is a social networking and identity service website owned and operated by Google, located at www.plus.google.com. Common features include the following:

- a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.
- b. Circles: Google+ allows users to establish “circles” which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical “Friends” list function used by sites such as Facebook and MySpace.
- c. Communities: Communities allow users with common interests to communicate with each other.
- d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.
- e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.
- f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.

14. Google Web and App History is a feature of Google Search in which a user’s search queries and results and activities on other Google services are recorded. This feature is only available for users logged into a Google account. A user’s Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.

15. Google Drive is a file storage and synchronization service provided by Google, located at www.drive.google.com. This service provides cloud storage, file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.

16. Google Android Backup is a service provided by Google to backup data connected to users' Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users' devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

EMAIL ACCOUNTS

17. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the account listed in Attachment A-2. Subscribers obtain accounts by registering with Google. During the registration process, Google requests potential subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. Based upon my training and experience, I am aware such information may constitute evidence of the subject crimes under investigation because the information can be used to identify the account's user or users.

18. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

19. Google subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. Based upon my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

20. Based upon my training and experience, email providers generally request their subscribers provide certain personal identifying information when registering for an email account. Such information typically includes the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Based upon my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know, even if subscribers insert false information to conceal their true identity, this information often provides clues to their actual identity, location, or illicit activities.

21. Based upon my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account

(such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often maintain records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

22. Based upon my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Based upon my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Based upon my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

AMINO

24. Amino is a free-access internet website and cellphone application created and managed by its parent company, Narvii, Inc., which is based in New York, New York. Amino features a network of both public and private groups directed and targeted at individuals over the age of 13 with various interests such as MLP, anime, Spongebob, etc. Amino features private chat functions which are not publicly accessible, making them less discoverable for third parties, including law enforcement.

25. Amino provides a variety of online services, including private communication access, to the general public. Subscribers obtain an account by registering with Amino online via the Amino website or via the Amino cell phone application. During the registration process, Amino requests potential subscribers to provide basic personal information. Since Amino's data and information is managed by Narvii, Inc., Narvii, Inc.'s computers are likely to contain stored electronic communications and other data, including retrieved and unretrieved chats, and information concerning subscribers and their use of Amino services, such as account access information, chat contents, and account application information. Based upon my training and experience, I am aware such information may constitute evidence of the subject crimes under investigation because said information can be used to identify the account's user or users.

26. Although users can create accounts on Amino and view other users' content free of charge, some of Amino's services require payment of fees. For example, licenses for users to utilize particular for-pay aspects of services such as "coins" requires payment. Coins allow users to purchase premium items such as custom chat bubbles and stickers in the virtual Amino store.

27. Amino maintains electronic records pertaining to subscriber accounts. These records include subscriber information, account access information, account application information, and user content (including image files) posted on Amino.

28. Narvii, Inc. stores data connected to Amino accounts for as long as that account is open (e.g., has not been deleted by its owner). If a user deletes their Amino account, Narvii, Inc. stores the associated content for up to 30 days before all data is removed from their systems. If a user manually deletes an individual piece of content, such as a chat message, the content will be deleted immediately and not saved past the time of deletion.

29. Social networking platforms like Amino typically retain other information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, IP addresses utilized to access the account and post content, and the means and source of any payments associated with the service (including any credit card or bank account numbers). In some cases, users may communicate directly with Amino about issues related to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Amino typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

FACTS IN SUPPORT OF PROBABLE CAUSE

BACKGROUND OF INVESTIGATION

30. On September 20, 2018, AFOSI 10 FIS received notification of the following information. During a March 2018 employment interview conducted by another federal agency, **SIT** disclosed he had previously communicated online with minor girls, accessed child pornography, and fantasized about raping minor girls. **SIT** did not specify the time period during which these purported activities and fantasies took place. **SIT** stated he communicated with certain girls he identified as "Hannah Hite" (a 14-year old from Virginia), and "Emma Nichols" (a 15-year old from Southern California) via Google Hangouts and Amino (see paragraph 9 for definitions). He further outlined evasive measures he took in order to conceal his identity and maintain anonymity when chatting with the minor girls. **SIT** further stated he began these communications through Google Hangouts, but later transitioned to Amino because he believed it was a more secure, less

discoverable means of communication. He explained he was motivated to move to Amino after learning about a man who was charged with crimes involving child pornography based upon evidence derived from Google Hangouts. **SIT** described his online conversations with said minor girls mainly revolved around their shared interest in MLP (see paragraph 9). **SIT** denied engaging in sexually explicit discussions and/or sending or receiving nude images with any minors on Amino. He relayed he discussed meeting said minor girls at MLP conventions (see paragraph 9). **SIT** further admitted he personally attended MLP conventions for several years, and further described how he fantasized about raping the minor girls he observed there. He opined the best time to abduct and rape the minor girls at these conventions would be during "the concert" portion of the convention, when the girls were observed running around without their parents. He indicated that he attended a MLP convention as recently as October 2018, and he remains actively and frequently engaged on social media.

31. During the interview of **SIT**, he stated he was sexually attracted to girls as young as 6 years old, but preferred 10-year olds, citing physiological aspects of their bodies consistent with that age group, such as little to no breast development and/or pubic hair. **SIT** described his thoughts of seeing minor girls crying in pain, in association with him having unauthorized contacts which he found nonetheless desirable. He further stated he had strong urges to have sex with minor girls, and detailed specific plans to engage in acts of "rape" with minor girls at both his workplace at the time, the Lumina Theater, 620 Market St., Chapel Hill, NC, and at his former place of worship, to wit: the Hillsong Church, 201 Culbreth Rd, Chapel Hill, NC. He described certain plans he envisioned which included specifics as to the location of surveillance cameras, and when the targeted girls in either location would likely be without the presence of their parents.

32. During the employment interview of **SIT**, he admitted to accessing child pornography through Ukrainian and Russian websites. **SIT** stated he was interested in accessing the so-called "Dark Web" because he heard it contains child pornography (see paragraph 9). He admitted he researched how to access the Dark Web during approximately the March 2017 time frame, when he was then 21 years old. He stated he did not download the relevant software to access the Dark Web because it was too difficult for him to figure out.

33. In April 2018, after said employment interview, but prior to AFOSI learning of **SIT**'s disclosures, **SIT** was hired as a civilian employee at WPAFB, OH. He currently is employed as a Health Physicist at a WPAFB nuclear waste facility. **SIT** resides at 5440 Cobb Dr., Dayton, OH, which is located in a privatized base housing area within a federal exclusive jurisdiction zone. His residence is adjacent to a Child Development Center, and is approximately 0.4 miles from Beverly Gardens Elementary School, 5555 Enright Ave., Riverside, OH. **SIT** has one roommate, 2Lt Anthony Lawrence Romett, who is stationed at the Air Force Research Laboratory at WPAFB, OH. **SIT** first met his roommate at the WPAFB housing office during the late March to early April 2018 time frame.

34. In September 2018, after receipt of the information contained in the March 2018 employment interview, AFOSI discovered that the Fairfax County, VA Police Department had previously opened an investigation concerning this matter in March 2018. They did not take any substantive criminal action because **SIT** no longer resided or was present in their jurisdiction. As a result, in September 2018, AFOSI assumed lead responsibility on this investigation.

35. In October 2018, AFOSI analysts conducted a review of **SIT**'s social media presence. This review determined **SIT**, operating under the username *Banquo0*, and had memberships in many

MLP websites. AFOSI analysts identified **juloischika@gmail.com** as one of **SIT**'s commonly-used email addresses. **SIT**'s Amino account was found to be associated with this email, **juloischika@gmail.com**, the user name **Banquo0**, and the account profile address <http://aminoapps.com/p/50nqz2>.

36. **SIT** listed a personal biography and his pony avatar Banquo on his public Amino page (see paragraph 9). Many of the details provided in his profiles appear to be autobiographical details, to include the fact he is currently looking for a significant other, and indicating he has "never had a SSP" before (SSP stands for "Special Some Pony," a term meaning significant other from the MLP television series). He self-identified on his Amino profile page as a "23 [year] old...Health Physicist" and further provided links to his known outside social media accounts on DeviantArt, Twitter, and YouTube (DeviantArt is a website on which users can publicly and privately share various forms of art). On the linked DeviantArt page, he identified himself as "Logan" and lists his date of birth as "October 9."

37. **SIT** was also found to have two Google+ profiles. One account is listed under the username "Logan Sit," and displays a photo of his face (found at plus.google.com/106609570102327977406). The other is listed under the username **Banquo0**, and displays his known MLP avatar as well as his email address, **juloischika@gmail.com** (found at plus.google.com/117651153278962826688).

38. Neither **SIT**'s Google contacts, nor his Amino contacts could be publicly discerned. Similarly, his private communications were unable to be publicly accessed. AFOSI analysts opined **SIT** likely utilized website private messaging functions to conceal his interactions. AFOSI additionally conducted a review of **SIT**'s U.S. Government email account which revealed another email address linked to **SIT**, to wit: **logansit@gmail.com**.

39. In support of AFOSI's investigation, on October 11, 2018 the Federal Bureau of Investigations (FBI) submitted administrative subpoenas for records associated with some of **SIT**'s known social media accounts. The information returned from the administrative subpoena of **SIT**'s Facebook account revealed the email address **logansit@gmail.com** was listed as his address when he registered for his account. Narvii, Inc. revealed **SIT**'s Amino account was opened on July 20, 2016. It also confirmed this account was registered to **juloischika@gmail.com**. This account was regularly accessed between October 1, 2017 and October 4, 2018. It has also been determined **SIT** accessed this Amino account a total of 901 times during said time period. Further research indicates as of December 18, 2018, **SIT** accessed his Amino account for 361 consecutive days. No accounts were registered with Amino associated with **SIT**'s other known email addresses. On November 26, 2018, AFOSI submitted a preservation request for **SIT**'s Amino account.

40. If **SIT** utilized Amino and Google Hangouts as the platforms on which he contacted the said minor girls as he disclosed during his March 2018 employment interview, **SIT** was then over the age of 18 at the time of those chats. Google Hangouts has only been in existence since May 2013, a few months prior to **SIT**'s 18th birthday. Google Hangouts was not widely used prior to February 2015, when Google merged their preceding communication platform, Google Talk, with Google Hangouts. The investigation has confirmed that **SIT** first opened his Amino account in July 2016, when he was 20 years old. Furthermore, the chat feature on Amino was first created in October 2014. Through extrapolation, the investigation confirmed this occurred prior to **SIT**'s 18th birthday.

EVIDENCE AVAILABLE IN EMAIL AND SOCIAL MEDIA ACCOUNTS

41. Based on my training and experience, I am aware individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via email, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

42. Based on my training and experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use the chat functions via these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

43. Based on my training and experience, I know individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

44. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.

45. Based on my training and experience, I know many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

46. As noted above, Narvii, Inc. and Google, LLC maintain various subscriber and user information that their users provide when registering for accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases

where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

47. Narvii, Inc. and Google, LLC maintain various logs of IP addresses utilized to access the accounts. The IP address information is again materially important in child pornography investigations. This information commonly helps in identifying the subjects and the locations where their computer devices are located.

48. Based on all of the information detailed above, there is probable cause to believe information associated with **SIT**'s Google and Amino accounts contain evidence of his illicit activities, as further defined in Attachment C.

49. As detailed above, the **juloischika@gmail.com** email address was used to register the **Banquo0** Amino account. As such, it is reasonable to believe the user of the **Banquo0** Amino account also uses the **juloischika@gmail.com** email address. Additionally, the **logansit@gmail.com** email address was listed to register **SIT**'s Facebook account. It is further reasonable to believe **SIT** also uses the **logansit@gmail.com** email address. Based on all of the information detailed above, there is probable cause to believe the information associated with the email accounts **juloischika@gmail.com** and **logansit@gmail.com** may contain additional evidence of the user's child pornography activities. Communications to or from these email accounts (including communications with adults or other third parties) may be materially relevant to the investigation, as these communications may help to corroborate the identity of the **Banquo0** account user. Furthermore, communications to and from these email accounts may contain discussions of child exploitation topics, the exchange of child pornography files, discussions with minors, and/or evidence of other electronic accounts utilized in furtherance of the child pornography activities.

EVIDENCE SOUGHT IN OTHER GOOGLE APPLICATIONS

50. Google has the ability to maintain information associated with the web and application history of its users. Such information is materially relevant in child exploitation investigations as it may help to identify websites used by subjects to obtain child pornography and locate victims.

51. Google Drive and Google Photos provide users with cloud computing, online file storage (as detailed above), and photo storage services. Based upon my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

52. Google Android Backup provides users with the ability to backup data on their cellphones and other electronic devices. Such data can be materially relevant in cases in which cellphones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities are no longer saved on the devices.

53. Google+ and Google Hangouts provides users with the ability to organize other users into groups for sharing information across various Google products and services. These applications facilitate individual and group chatting both in an instant messaging format and in a video chatting format. This data is materially relevant to this case as it may help identify, and/or provide evidence of communications with, other offenders and/or victims.


CONCLUSION

54. Based upon the aforementioned information, I respectfully submit there is probable cause to believe evidence, fruits, and instrumentalities of the criminal offenses listed in Attachment C may be located in the accounts described in Attachments A-1 and A-2. I, therefore, respectfully request the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.

REQUEST FOR SEALING

55. I further request the Court order all papers associated with this application, including the supporting Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the target an opportunity to flee from prosecution, destroy, or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation; therefore, the United States requests, pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Narvii, Inc. and Google, LLC be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this search warrant for such period as the Court deems appropriate.

Respectfully submitted,


SPECIAL AGENT TEDDI D. RACHELL
AIR FORCE OFFICE OF SPECIAL
INVESTIGATIONS

Sworn and subscribed before me on this 28th day
of December, 2018.


MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE